

**Legislative History for
University Policy 3-234 Revision 7 Building Access and Surveillance
Systems
&
University Rule 3-234A Revision 0 Building Access and Surveillance
Systems**

Approved by the Academic Senate January 7, 2019.

Approved by the Board of Trustees, March 12, 2019
With designated effective date of the date of final approval—March 12, 2019

Prepared by Bob Flores, Senate Policy Liaison, for the Institutional Policy Committee.

Contents:

- Explanatory memorandum to Senate, dated January 7, 2019
- Explanatory memorandum to Senate, dated October 30, 2018
- Policy 3-234 Revision 7, as finally approved.
- Rule 3-234A Revision 0, as finally approved.
- University Procedure 3-234A (example only-- draft 2018-10-29)
- Slide Presentation to Senate November 5, 2018

Memorandum

From: Bob Flores, Senate Policy Liaison – for the Executive Committee’s appointed ad hoc drafting committee.

To: Academic Senate, for meeting of **January 7, 2019**

Re: Update on Proposal for Policy 3-234 and Rule 3-234A – Building Access and Surveillance Systems

This proposal was presented on the Notice of Intent Calendar at the Senate meeting of November 2018, and it now returns on the January 2019 Debate Calendar for a vote of approval. At the November meeting and again at the December meeting, Senate members were invited to provide input for improvements in the proposal, members of the Senate Executive Committee have had multiple opportunities to provide input, members of the Institutional Policy Committee have been consulted repeatedly, and other members of the University community have similarly been invited to give input during the intervening months. Extensive input was received, and as a result we have made several significant changes in the text of the proposed Policy 3-234. This memorandum for January 7 explains the changes made since November. The contents of the proposal as of November were described in the memorandum presented at the November meeting, and a copy of that earlier memorandum is attached below for your convenience.

The Senate is now asked to approve the contents of the proposed Policy 3-234, and the accompanying proposed Rule 3-234, both of which are included in the agenda materials for this proposal.

All of the text changes in the draft Policy made since the version presented at the November meeting are clearly marked with ~~redline~~/ underline font markings, those parts which will be of particular interest are marked with highlighting, and margin comments are included to explain some of those most significant changes. And for your convenience, here are descriptions of the more significant changes.

A. Expanding the permissible uses of surveillance data—beyond criminal activity.

The most important changes are to follow through on a set of issues that were mentioned in the earlier draft, and were described and discussed at the Senate meetings in November and December. They involve balancing of concerns for individual privacy, with concerns for providing a campus environment that is safe for members of the University community, protecting University resources, and complying with various regulatory requirements. In the earlier draft it was stated that data gathered from surveillance systems would primarily be usable only to detect and deter *criminal* activity. The extensive input we received strongly recommended that the permissible uses be expanded to include situations where there might not be activity that would be technically defined by state or federal law as *crimes*--- but which nevertheless would be of great concern for members of the University community.

In response, we revised the draft Policy to include a list of other situations, not involving criminal activity, for which use of surveillance data could potentially be authorized. However, those other types uses are not freely permitted—each other type of use will only be allowed if explicitly approved in advance through an authorization process which requires approval by the newly established Surveillance Systems Administrators Committee (with representatives of the faculty, students, and staff,

as well as administrative officers). And each such authorization of uses for situations not limited to criminal activity must be periodically reported to the Senate.

That newly added list of potentially permissible uses includes:

- An administrative investigation of a potential violation of a *non-criminal law or external regulation* which is directly applicable to the University or University personnel, if such a violation presents a substantial risk of serious harm to the University or any individual (e.g., federal or state regulations regarding storage of controlled substances, or hazardous materials).
- An administrative investigation of a potential violation of a *University Regulation* involving a type and degree of non-criminal misconduct which presents a substantial risk of serious harm to the University or an individual (e.g., posting racially derogatory materials in a University work- or learning-space to create a hostile work/ learning environment for University employees or students; or operating or storing a wheeled riding device in a dangerous manner or in a prohibited zone).
- An administrative investigation by a student-services office regarding a potential disappearance of a campus-resident student, in circumstances in which the student may be at risk of serious harm (e.g., a student housing administrator investigating concerns of a minor student's family about the student's well-being after a long period without contact).
- A practice of routinely monitoring the presence of University employees or other individuals in specific locations of a facility of the University Hospitals and Clinics, for the limited purposes of protecting patient safety and ensuring compliance with applicable safety regulations.
- A practice of routinely monitoring the presence of University employees or other individuals in specific locations of a University facility with restricted access, in circumstances in which such monitoring is necessary to comply with directly applicable external laws and regulations or University Regulations such as for protection of sensitive data or regulated technology, or control of special materials (e.g., University Policy 4-004 Information Security; Policy 7-007 Export Control Compliance; Policy 3-300 University Health and Safety).

B. Allowing use of facial recognition software in limited circumstances.

The earlier draft categorically prohibited the use of facial recognition software to track an individual on campus. The revised draft will allow such technology to be used but only in a very limited set of circumstances: “The University will not use facial recognition computer software or equivalent information technology to process video surveillance data to track the presence at a campus location of a particular person for any purpose **other than addressing criminal activity which presents a substantial risk of serious harm to the University or an individual (e.g., a credible threat of a terrorist attack by an identifiable individual at a high-population event on campus).**”

C. Changes regarding retention periods for surveillance data.

The earlier draft included a specified period of time to retain certain types of surveillance data (before automatically deleting the data). We realized such a fine level of detail is inappropriate to include in the main Policy—and should instead be left to be developed by the new SSAC—oversight committee. So that detail is deleted from the revised draft, and instead the SSAC is assigned the task of developing appropriate procedures with specified retention periods for various types of surveillance data.

D. Allowing surveillance systems to be operated by non-University employees—in limited circumstances.

The earlier draft stated that only University employees could be allowed to operate surveillance systems. We received input from the Hospitals and Clinics explaining that in a few instances the University contracts with vendors to operate surveillance systems, at locations of clinics away from the University main campus. The new draft is revised to allow for such contractor-operated systems at off-site locations---but requires that each such contractor-operated system be registered with and approved by the SSAC, to ensure that those contractor-operated systems are operated in accord with the same general privacy-protective principles that apply to systems which are operated by University employees.

--end--

[See October 2018 memo attached for reader convenience]

Memorandum

From: Bob Flores, Senate Policy Liaison – for the Executive Committee’s appointed ad hoc drafting committee.

To: Academic Senate

Re: Updated Proposal for Policy 3-234 and Rule 3-234A – Building Access and Surveillance Systems

Date: **October 30, 2018** [for the November Senate meeting]

I. Overview:

This is a proposal to retitle and replace existing contents of Policy 3-234 Key Policy with a combination of revised Policy 3-234 Building Access and Surveillance, and new Rule 3-234A Building Access and Surveillance.

Recent developments—input from the Executive Committee and an ad hoc drafting committee.

The proposal project has been underway since early 2018. A version which had been approved through the usual policy development process, including approval at the vice-presidential level, was presented to the Senate Executive Committee September 17. EC members identified numerous concerns about the protections of privacy in the proposal, and the EC determined that it would need substantial further review and likely revision before being brought to the Senate for formal approval. The EC appointed two EC faculty members with expertise in privacy law (Randy Dryer—Law, Leslie Francis—Law) to join with the Senate Officers and work with the existing drafting committee members, to serve as an ad hoc drafting committee, to address the concerns and develop a revised proposal ready for presentation to the Senate. At the October Senate meeting an overview of the project was presented and members were invited to provide input (and from that student representative Devon Cantwell was added to the ad hoc committee). Further discussion took place at the October 15 EC meeting. Numerous drafts have been produced and reviewed within the ad hoc committee, leading up to the proposal now being submitted for the November 5 Senate meeting on the “Intent Calendar.”

The proposal now presented includes (i) explanatory memo; (ii) Policy 3-234 draft, (iii) Rule 3-234A draft, and (iv) an example of a University Procedure 3-234 (providing an example of a formal Procedure which would be approved and implemented by the “SSAC” committee which is proposed to be created).

On request of the EC, the Policy includes a specific provision requiring that the new regulatory system and contents of the Regulations be reviewed in year 2020 and a report with recommendations be presented to the Academic Senate by October 2020. This will ensure an opportunity for revising of the Regulations as may be needed based on experience over a startup period. The Policy will also require ongoing annual reporting to the Senate, and provides a mechanism for any person concerned about operation of a surveillance system to bring a concern about privacy to the Senate President and in turn to the Senate Executive Committee, at any time.

And it is clarified that this current Policy and Rule are focused on primarily *fixed-location* surveillance systems—permanently associated with a particular space. There will subsequently be developed other regulations provisions to address primarily *mobile* systems, such as drone cameras or body-worn cameras.

II. Background.

The proposed set of Policy and Rule will replace the previous Policy 3-234 Key Policy. That existing Policy's content was developed at a time when the technology for controlling access to buildings and interior spaces consisted only of mechanical locks and physical keys, and when there was no widespread usage of video cameras or other surveillance systems. That content had not been updated in more than 20 years. In these past two decades, building access and campus security technologies and practices have evolved to include electronic door locks and pervasive camera surveillance systems. The existing 3-234 is completely inadequate to address issues arising with the newer technology, and other regulations do not adequately address the multitude of important issues. The modern rapidly spreading use of electronic door controls and surveillance systems which collect images and other electronic data is raising privacy concerns—which should be but until now have not been addressed in regulations.

The proposal is to update the contents of our regulations to reflect the current extensive and anticipated even more extensive usage of the modern technologies—through a regulatory system that will recognize and appropriately balance issues of privacy, and of campus safety and security. The archaic existing Policy contents would be replaced with a combination of a greatly revised Policy, one associated Rule for now (and likely other Rules to come later), and authorize a new committee to promulgate additional guidance documents with further details.

III. Highlights of the revised Policy

- A comprehensive regulatory system will be established, regulating most of the building access systems and video surveillance systems which are operated by the University on the main Salt Lake campus, and at other satellite campus areas controlled by the University.
- The new Surveillance Security Administrators Committee will be created to serve as the primary oversight body for that regulatory system. It will be assigned broad responsibilities to establish and implement oversight procedures. The SSAC will be comprised of administration representatives (including Public Safety, Office of General Counsel, and Facilities Management). And as specifically requested by the EC, it will include two representatives of the faculty (selected by the Senate Personnel & Elections Committee), and representatives of staff and students.
- As the most important long term component--- all existing building access and surveillance systems, and any new systems, will be required to be registered with and approved through the regulatory system overseen by the SSAC, and will then be periodically reviewed for re-approval. The SSAC will develop and implement a reasonable timeline for the registration process, and a comprehensive set of review criteria which must be consistent with certain fundamental principles already specified in the proposed Regulations.
- Exemptions from the registration & approval requirement will be grantable for some types of small-scale access & surveillance systems which are not appropriate for the University-wide regulatory system.
- The regulatory system will recognize differences between the centrally-operated systems which typically are installed in more open public areas, and smaller systems installed in specific buildings or smaller sections of buildings and operated locally by specific departments. Both types will be regulated under generally similar criteria, but with variations as appropriate for the various types of systems.

- Once the registration and regulatory system is implemented, collecting of surveillance data will only be allowed by systems which have been registered and approved (unless specifically exempted).
- The SSAC will develop and implement a set of criteria for the training, qualifications, and regular oversight of system operations personnel, and only such qualified personnel will be allowed to operate systems and thereby have routine maintenance access to stored surveillance data.
- The storage of surveillance data will be very highly restricted—retention periods will be imposed by the SSAC, and data storage systems must meet security criteria and other design criteria established by the SSAC.
- The regulatory system will balance concerns of safety and security and concerns of privacy. The placement of surveillance systems and the uses of surveillance data by University offices & personnel will be very highly restricted. In general, the University will only use surveillance data for furthering campus safety and security—deterring and detecting criminal activity, to protect members of the University community and lawful visitors, and prevent property theft or damage.
- In particular, there will be *restrictions on*: collecting of audio surveillance data with discernable human voices (i.e., no monitoring of contents of conversations); use of facial recognition software to track persons; and video surveillance of essentially private spaces such as faculty & staff individual offices, bathrooms, etc.
- Some limited exceptions to the above tight restrictions on use will be possible only with specific advance approval of the SSAC and the Office of General Counsel.
- Without exception—the University will not use surveillance data to monitor a student’s course attendance or an employee’s compliance with workplace attendance requirements.
- Regular users of particular spaces should be consulted when systems are being considered for initial installation—e.g., employees and students of a department should be consulted when a system is being considered for the space occupied by that department.
- Appropriate signage must be installed to alert occupants of the presence of surveillance systems.
- Operation of systems and storage and use of surveillance data must be in compliance with various applicable federal laws which address individual privacy and campus safety—including the Family Educational Rights and Privacy Act (FERPA) regarding student records, the CLERY Act regarding campus safety and security, the Health Insurance Portability and Accountability Act (HIPAA) regarding health care patient information
- It is recognized that under the Utah Governmental Records Access and Management Act (GRAMA), the University is defined as a governmental entity, and University records, including stored surveillance data, are governmental records, which may be subject to public records requests. The Policy recognizes that the University must comply with GRAMA when records requests are made—but affirms that the University will protect individual privacy to the fullest extent possible under the applicable law in such cases.
- Academic researchers, including University personnel conducting academic research, may request access to stored surveillance data—and such requests will be processed under the terms of GRAMA—in which case the Policy affirms that the University will also protect individual privacy to the fullest extent possible under the applicable law. Research in such cases would also be subject to typical requirements for research involving human subjects—such as review by the Institutional Review Board.

IV. Highlights of the new Rule.

- The Rule addresses managerial issues for building access and surveillance systems, including the methods for funding of initial installation and then ongoing maintenance, and the responsibilities for operations.
- For legacy technology of manually operated mechanical locks and keys, the Rule provides for methods of issuing regular keys and master keys, allocating costs for keys, and processes for re-keying necessitated by loss of control over keys.
- In accord with a provision in the main Policy allowing for exemption of some types of surveillance systems from the ordinary registration and approval process—the Rule specifies certain types of systems/ uses which will typically be exempted (as will be further described by the SSAC).

V. The Example of an SSAC-developed *University Procedure*.

This document is included in the proposal as means of showing Senate members how the SSAC is likely to proceed with implementing the new regulatory process. It describes a potential approach to setting a timeline for surveillance systems to be registered—possibly on a staggered schedule. It has an example of a checklist such as the SSAC will develop and use for reviewing and approving surveillance systems which are to be registered.

VI. Consultation and Approvals.

Prior to the presentation to the Senate Executive Committee and the appointment by the EC of an ad hoc committee which then substantially revised the proposal, the proposal had been developed over most of year 2018 by a team including Police Chief Dale Brophy, Facilities Management Executive Director Cory Higgins, and Senate Policy Liaison Bob Flores. It had been reviewed through the Institutional Policy Committee (on multiple occasions), the Office of General Counsel, and the President’s Executive Leadership Team. It had been approved by Vice President for Administrative Services John Nixon.

It has subsequently been very substantially revised with involvement of the EC appointed ad hoc committee. Subsequent to Senate approval, it will ultimately be presented for final approval of the University President and the Board of Trustees.

It is proposed that the revised/new regulations take effect immediately upon final approval.

Questions about the proposal may be addressed to:

Bob Flores, Senate Policy Liaison robert.flores@law.utah.edu

~~Cory Higgins, c/o Executive Assistant Karen Janicki, Facilities Management
(801) 581-7389 karen.janicki@fm.utah.edu~~

Memorandum

From: Bob Flores, Senate Policy Liaison – for the Executive Committee’s appointed ad hoc drafting committee.

To: Academic Senate

Re: Updated Proposal for Policy 3-234 and Rule 3-234A – Building Access and Surveillance Systems

Date: October 30, 2018

I. Overview:

This is a proposal to retitle and replace existing contents of Policy 3-234 Key Policy with a combination of revised Policy 3-234 Building Access and Surveillance, and new Rule 3-234A Building Access and Surveillance.

Recent developments—input from the Executive Committee and an ad hoc drafting committee.

The proposal project has been underway since early 2018. A version which had been approved through the usual policy development process, including approval at the vice-presidential level, was presented to the Senate Executive Committee September 17. EC members identified numerous concerns about the protections of privacy in the proposal, and the EC determined that it would need substantial further review and likely revision before being brought to the Senate for formal approval. The EC appointed two EC faculty members with expertise in privacy law (Randy Dryer—Law, Leslie Francis—Law) to join with the Senate Officers and work with the existing drafting committee members, to serve as an ad hoc drafting committee, to address the concerns and develop a revised proposal ready for presentation to the Senate. At the October Senate meeting an overview of the project was presented and members were invited to provide input (and from that student representative Devon Cantwell was added to the ad hoc committee). Further discussion took place at the October 15 EC meeting. Numerous drafts have been produced and reviewed within the ad hoc committee, leading up to the proposal now being submitted for the November 5 Senate meeting on the “Intent Calendar.”

The proposal now presented includes (i) explanatory memo; (ii) Policy 3-234 draft, (iii) Rule 3-234A draft, and (iv) an example of a University Procedure 3-234 (providing an example of a formal Procedure which would be approved and implemented by the “SSAC” committee which is proposed to be created).

On request of the EC, the Policy includes a specific provision requiring that the new regulatory system and contents of the Regulations be reviewed in year 2020 and a report with recommendations be presented to the Academic Senate by October 2020. This will ensure an opportunity for revising of the Regulations as may be needed based on experience over a startup period. The Policy will also require ongoing annual reporting to the Senate, and provides a mechanism for any person concerned about operation of a surveillance system to bring a concern about privacy to the Senate President and in turn to the Senate Executive Committee, at any time.

And it is clarified that this current Policy and Rule are focused on primarily *fixed-location* surveillance systems—permanently associated with a particular space. There will subsequently be developed other regulations provisions to address primarily *mobile* systems, such as drone cameras or body-worn cameras.

II. Background.

The proposed set of Policy and Rule will replace the previous Policy 3-234 Key Policy. That existing Policy's content was developed at a time when the technology for controlling access to buildings and interior spaces consisted only of mechanical locks and physical keys, and when there was no widespread usage of video cameras or other surveillance systems. That content had not been updated in more than 20 years. In these past two decades, building access and campus security technologies and practices have evolved to include electronic door locks and pervasive camera surveillance systems. The existing 3-234 is completely inadequate to address issues arising with the newer technology, and other regulations do not adequately address the multitude of important issues. The modern rapidly spreading use of electronic door controls and surveillance systems which collect images and other electronic data is raising privacy concerns—which should be but until now have not been addressed in regulations.

The proposal is to update the contents of our regulations to reflect the current extensive and anticipated even more extensive usage of the modern technologies—through a regulatory system that will recognize and appropriately balance issues of privacy, and of campus safety and security. The archaic existing Policy contents would be replaced with a combination of a greatly revised Policy, one associated Rule for now (and likely other Rules to come later), and authorize a new committee to promulgate additional guidance documents with further details.

III. Highlights of the revised Policy

- A comprehensive regulatory system will be established, regulating most of the building access systems and video surveillance systems which are operated by the University on the main Salt Lake campus, and at other satellite campus areas controlled by the University.
- The new Surveillance Security Administrators Committee will be created to serve as the primary oversight body for that regulatory system. It will be assigned broad responsibilities to establish and implement oversight procedures. The SSAC will be comprised of administration representatives (including Public Safety, Office of General Counsel, and Facilities Management). And as specifically requested by the EC, it will include two representatives of the faculty (selected by the Senate Personnel & Elections Committee), and representatives of staff and students.
- As the most important long term component--- all existing building access and surveillance systems, and any new systems, will be required to be registered with and approved through the regulatory system overseen by the SSAC, and will then be periodically reviewed for re-approval. The SSAC will develop and implement a reasonable timeline for the registration process, and a comprehensive set of review criteria which must be consistent with certain fundamental principles already specified in the proposed Regulations.
- Exemptions from the registration & approval requirement will be grantable for some types of small-scale access & surveillance systems which are not appropriate for the University-wide regulatory system.
- The regulatory system will recognize differences between the centrally-operated systems which typically are installed in more open public areas, and smaller systems installed in specific buildings or smaller sections of buildings and operated locally by specific departments. Both types will be regulated under generally similar criteria, but with variations as appropriate for the various types of systems.

- Once the registration and regulatory system is implemented, collecting of surveillance data will only be allowed by systems which have been registered and approved (unless specifically exempted).
- The SSAC will develop and implement a set of criteria for the training, qualifications, and regular oversight of system operations personnel, and only such qualified personnel will be allowed to operate systems and thereby have routine maintenance access to stored surveillance data.
- The storage of surveillance data will be very highly restricted—retention periods will be imposed by the SSAC, and data storage systems must meet security criteria and other design criteria established by the SSAC.
- The regulatory system will balance concerns of safety and security and concerns of privacy. The placement of surveillance systems and the uses of surveillance data by University offices & personnel will be very highly restricted. In general, the University will only use surveillance data for furthering campus safety and security—deterring and detecting criminal activity, to protect members of the University community and lawful visitors, and prevent property theft or damage.
- In particular, there will be *restrictions on*: collecting of audio surveillance data with discernable human voices (i.e., no monitoring of contents of conversations); use of facial recognition software to track persons; and video surveillance of essentially private spaces such as faculty & staff individual offices, bathrooms, etc.
- Some limited exceptions to the above tight restrictions on use will be possible only with specific advance approval of the SSAC and the Office of General Counsel.
- Without exception—the University will not use surveillance data to monitor a student’s course attendance or an employee’s compliance with workplace attendance requirements.
- Regular users of particular spaces should be consulted when systems are being considered for initial installation—e.g., employees and students of a department should be consulted when a system is being considered for the space occupied by that department.
- Appropriate signage must be installed to alert occupants of the presence of surveillance systems.
- Operation of systems and storage and use of surveillance data must be in compliance with various applicable federal laws which address individual privacy and campus safety—including the Family Educational Rights and Privacy Act (FERPA) regarding student records, the CLERY Act regarding campus safety and security, the Health Insurance Portability and Accountability Act (HIPAA) regarding health care patient information
- It is recognized that under the Utah Governmental Records Access and Management Act (GRAMA), the University is defined as a governmental entity, and University records, including stored surveillance data, are governmental records, which may be subject to public records requests. The Policy recognizes that the University must comply with GRAMA when records requests are made—but affirms that the University will protect individual privacy to the fullest extent possible under the applicable law in such cases.
- Academic researchers, including University personnel conducting academic research, may request access to stored surveillance data—and such requests will be processed under the terms of GRAMA—in which case the Policy affirms that the University will also protect individual privacy to the fullest extent possible under the applicable law. Research in such cases would also be subject to typical requirements for research involving human subjects—such as review by the Institutional Review Board.

IV. Highlights of the new Rule.

- The Rule addresses managerial issues for building access and surveillance systems, including the methods for funding of initial installation and then ongoing maintenance, and the responsibilities for operations.
- For legacy technology of manually operated mechanical locks and keys, the Rule provides for methods of issuing regular keys and master keys, allocating costs for keys, and processes for re-keying necessitated by loss of control over keys.
- In accord with a provision in the main Policy allowing for exemption of some types of surveillance systems from the ordinary registration and approval process—the Rule specifies certain types of systems/ uses which will typically be exempted (as will be further described by the SSAC).

V. The Example of an SSAC-developed University Procedure.

This document is included in the proposal as means of showing Senate members how the SSAC is likely to proceed with implementing the new regulatory process. It describes a potential approach to setting a timeline for surveillance systems to be registered—possibly on a staggered schedule. It has an example of a checklist such as the SSAC will develop and use for reviewing and approving surveillance systems which are to be registered.

VI. Consultation and Approvals.

Prior to the presentation to the Senate Executive Committee and the appointment by the EC of an ad hoc committee which then substantially revised the proposal, the proposal had been developed over most of year 2018 by a team including Police Chief Dale Brophy, Facilities Management Executive Director Cory Higgins, and Senate Policy Liaison Bob Flores. It had been reviewed through the Institutional Policy Committee (on multiple occasions), the Office of General Counsel, and the President’s Executive Leadership Team. It had been approved by Vice President for Administrative Services John Nixon.

It has subsequently been very substantially revised with involvement of the EC appointed ad hoc committee. Subsequent to Senate approval, it will ultimately be presented for final approval of the University President and the Board of Trustees.

It is proposed that the revised/new regulations take effect immediately upon final approval.

Questions about the proposal may be addressed to:

Bob Flores, Senate Policy Liaison robert.flores@law.utah.edu

Cory Higgins, c/o Executive Assistant Karen Janicki, Facilities Management
(801) 581-7389 karen.janicki@fm.utah.edu

Policy 3-234: Building Access and Surveillance Systems. Revision 7.

Effective Date: [Upon final approval]

{Drafting note. For Revision 7, the entire contents of former Policy 3-234 Key Policy Revision 6 (shown below at the end with strikethrough font) are being deleted and replaced by the following entirely new contents, with the new title of Building Access and Surveillance Systems}

I. Purpose and Scope:

- A. Purpose: This Policy and associated Regulations regulate the installation and maintenance of building access systems and area surveillance systems in buildings and outdoor areas owned or controlled by the University of Utah, and regulate the collection, storage, disposal, access, and use of surveillance data from those systems.

*[The Surveillance System Administrator Committee (as defined below) shall during spring 2020 review this Policy and the system registration process it creates, and present to the Academic Senate by October 2020 a report with recommendations, including any recommendations for revision of this Policy and associated Regulations. **The report shall be provided to the Board of Trustees.** Further, as provided in this Policy, the SSAC shall also thereafter at least annually present a report to the Senate.]*

- B. Scope: The provisions of this Policy regulating installation and maintenance of building access systems and surveillance systems apply for all buildings or outdoor areas controlled by the University (except for premises leased to and controlled and occupied by non-University entities). These covered areas include all locations where the University of Utah Department of Public Safety has a security presence and responsibility. The provisions of this Policy regulating collection, storage, disposal, access, and use of surveillance data apply to all University departments and contracted entities conducting University activities, regardless of location.

[Drafting note: Responding to questions raised about buildings in Research Park which are the regular work sites for various University departments, this revised Scope description is intended to clarify that these same regulations apply to those University-occupied facilities in Research Park (or similar locations away from the main campus) as apply for facilities on main campus. The SSAC will be making available to those departments further information regarding the building access systems and surveillance systems in those areas which are operated by the University and are therefore directly governed by this Policy. The SSAC will also be gathering and sharing information regarding any systems deployed in such areas which are not operated by the University but instead controlled by a third-party (e.g., a landlord), and such research may lead to revisions of this Policy or changes in University

practices in negotiation of terms of leases regarding surveillance of University personnel being conducted by non-University entities.]

[User note: *This Policy and its associated Rules replace the former University Key Policy 3-234, as of 2019.* The current version of this Policy is primarily intended to regulate surveillance systems that are of primarily *fixed locations*. It is anticipated that a revised regulation will subsequently be developed regarding University surveillance systems which are primarily *mobile*, including cameras mounted on Unmanned Aircraft (i.e., drones, see Utah Code Ann. 72-14-101), and wearable camera devices operated by Department of Public Safety personnel (i.e., body cameras). Contact the Department of Public Safety for further information. Also there may be subsequent development of a regulation regarding special-purpose surveillance systems temporarily deployed for short-term events, such as events involving gatherings of large crowds.].

II. Definitions:

For the limited purposes of this Policy and any associated Regulations, these words and phrases have the following meanings:

- A. Approving Officer – A University officer holding the position of Department Head or higher.
- B. Building Access System –Key System (consisting of mechanical locks and keys, including master keys), and other devices, including an Electronic Access System, utilized to control access to a door or an area.
- C. Campus Building Access Team– The team within the Facilities Management Department (reporting to the Vice President of Administrative Services) that provides the central administration of the integrated surveillance and access systems for general campus and DPS-designated Public Safety Spaces.
- D. Criminal activity— Conduct which is punishable under the criminal laws applicable for the locations and persons involved—including the Utah Criminal Code and applicable federal law for activity occurring in Utah, and the laws of the applicable jurisdiction for activity occurring outside of Utah.
- E. DPS – Department of Public Safety – The University of Utah department incorporating campus police and security services.
- F. Electronic Access Control System – The hardware and software that control door access.

- G. Electronic Access Control Operator – An approved University employee who manages access rights of users through the Electronic Access Control System.
- H. [[Facility Steward – The facilities department or person with primary stewardship responsibility for a particular building or area.]] *{Drafting note: this defined term may be changed as needed as an editorial correction, upon approval of the chairperson of the SSAC, with notice to the Institutional Policy Committee.}*
- I. General Fund – The University’s general operating budget funded through state, tuition, and other sources.
- J. Public Safety Space – An indoor or outdoor space that is accessible to the general public and is designated by DPS as a public safety space based on a determination of significant potential risks for criminal activity.
- K. SSAC – Surveillance System Administrators Committee– A committee established under authority of this Policy with assigned responsibilities for implementation of this Policy and associated Regulations.
- L. Surveillance Data – Any electronic, printed, audible, visible or other form of information captured by a Surveillance System, including any record of user access generated through a Building Access System
- M. Surveillance System – A system capable of monitoring and recording the presence or activity of persons in a given physical area of a University building or outdoor area. **[This does not include an employee time clock system through which specific employees are required to register their presence at a work-site, for the specific purpose of tracking their work hours; and the data regarding employee presence collected through such a system is not considered Surveillance Data for purposes of this Policy.]** The current version of this Policy is intended to regulate systems which are of *primarily fixed locations*, not including systems which are *primarily mobile*. **[User note: it is anticipated that a revised regulation will subsequently be developed regarding University surveillance systems which are primarily mobile, such as body cameras, drones, etc.]**
- N. Surveillance System Device –A camera, microphone, video or audio data recording equipment, key card reader, or other type of device which is a component of a Surveillance System.

III. Policy:

A. Surveillance System Administrators Committee (SSAC).

The SSAC is hereby established as a University Committee. Its membership and leadership shall be appointed by the President of the University. Members shall include: (i) appropriate representation, as determined by the President, from among the following (or equivalent offices): Campus Building Access Team, the Department of Public Safety, the Office of General Counsel, the offices of the Senior Vice Presidents for Academic Affairs or Health Sciences, Hospitals and Clinics administration, and the office of the Vice President for Student Affairs; (ii) a representative of staff employee interests (selected in consultation with the Staff Council); (iii) a representative of student interests (selected in consultation with the Associated Students of the University of Utah); and (iv) **two Tenure-line or Career-line representative(s) of the University faculty recommended to the President by the Senate Personnel and Elections Committee, who shall serve for terms of three-years and may be recommended and reappointed for additional terms without limitation. The President of the Academic Senate, or designee(s), may substitute as needed in the absence of the faculty representatives.**

The SSAC shall have the functions described in this Policy and associated Regulations and otherwise assigned by the President. It shall receive administrative support from and regularly report to the Vice President for Administrative Services (or equivalent). **At least annually a summary report of the SSAC's recent activities shall be presented for the information of the Academic Senate. In addition, any member of the SSAC may at any time inform the Senate President, who may in turn inform the Senate Executive Committee, of any significant concern regarding any activities overseen by the SSAC, including a concern of inadequate protection of privacy of individual members of the University community.**

B. Registration, approval, installation and operation of building access systems and other surveillance systems.

1. General provisions.

a. There are broadly two categories of building access systems and other surveillance systems in use at the University:

(i) main central systems which are operated centrally under auspices of the Campus Building Access Team, typically controlling access to or surveilling designated Public Safety Spaces, transit hubs, and other general usage campus areas, and

(ii) systems which are dispersed among various buildings and facilities in various locations of the campus, with each system being operated under auspices of a particular Facility Steward responsible for the particular building or facility.

Systems of both categories must only be operated in accord with the fundamental principles underlying this Policy. To ensure enforcement of that requirement for the various dispersed systems, the University establishes and charges the SSAC to oversee a central registry and approval process for such systems.

2. Central registry and approval of building access systems and other surveillance systems.

a. The University will maintain a central registry and approval process for building access systems and other surveillance systems, which will be administratively situated within an office reporting to the Vice President for Administrative Services (or equivalent), and will operate under oversight of the SSAC. **The SSAC shall develop procedures and criteria for the systems registry and approval process, consistent with this Policy, including a timetable with deadlines for registration** of various types of systems.

b. Each unit of the University operating any building access system or other surveillance system shall by the established deadline submit an application for registration and approval of that system (unless exempted in accord with this Policy and associated Regulations). This includes any system purchased or installed directly by any department, as well as any system provided through third parties. After the established deadline, unless exempted, **no unit or person shall operate any pre-existing or any new building access system or other surveillance system at the University, or continue to store or use any surveillance data collected through such a system, unless the system has been registered and approved according to the SSAC-approved procedures.**

c. **Certain systems, or particular uses for surveillance systems may be exempted** from this registration and approval requirement, consistent with the purposes of this Policy, as shall be further described either in a University Rule associated with this Policy, or described in a University Procedure **approved by the SSAC.**

d. For each registered and approved system, the [Facility Steward] (or equivalent responsible position) **shall periodically provide updated**

information about the operation and monitoring of the system, at a time determined by the SSAC, and the system shall be reviewed for renewal, on a schedule determined by the SSAC (ordinarily no less frequently than every five years). The SSAC has full discretion to require a review of any system at any time, including in response to a concern about improper operation reported by any concerned person. A review shall be based on the then-current approval criteria.

e. After any review, if the SSAC finds that a system is not in substantial compliance with the then-current approval criteria, the SSAC may require that operation of the system be ceased. **A decision of the SSAC regarding approval, or cessation of operations of any system, is subject only to an appeal to the Vice President for Administrative Services (or equivalent officer), whose decision is final.**

f. The SSAC shall develop and implement a set of criteria for determining which University employee positions and individual employees shall be authorized to operate surveillance systems or access University surveillance data for University purposes, including criteria for training of employees for such specific responsibilities, and for auditing of compliance, and it shall include in the registry a current list of such authorized personnel.

g. The central registry, and the periodic regular reports of the SSAC, shall be considered public records, reviewable on request of any member of the University community in accord with the Government Records Access Management Act, except to the extent that the Office of General Counsel determines that any particular contents of such records should be redacted in accord with applicable provisions of GRAMA.

C. Principles and criteria for approval and ongoing operation of building access and surveillance systems.

The following principles, restrictions, and other criteria apply for those dispersed systems operated under auspices of a particular [Facility Steward] which are required to be registered and approved through the central registry described in Part III-B above, and the approval process shall ensure compliance with these requirements. **Unless otherwise indicated, they also apply for main central building access and surveillance systems which are operated centrally under auspices of the Campus Building Access Team.**

1. Principles for operation of building access and other surveillance systems, and collection, storage, disposal, access, and use of surveillance data.

- a. As an institution of higher education, including academic health sciences, with multiple missions, it is **a fundamental principle that the University recognizes and respects rights of privacy of individual persons** who enter various areas of the University campus to participate in University activities, including students, faculty members and staff employees, health care patients, and guest visitors entering for lawful purposes. It is also fundamental that the University seeks to ensure for all such persons a campus **environment that is safe from criminal activity and other causes of harm to their persons or loss or damage of their personal property**. And as a steward of public resources, the University seeks to prevent **loss or damage of University controlled property** resulting from criminal activity or other causes. The University regulates and operates building access systems and other surveillance systems so as to best serve the combined objectives—**balancing personal privacy, security and safety, and resource protection**.
 - b. **University personnel are required to operate such systems in compliance with applicable federal, state, and local law and in accord with University Regulations. This Policy and associated University Regulations shall be interpreted to comply with such applicable laws, whether currently existing or subsequently enacted, including federal and state constitutional provisions, the Family Educational Rights and Privacy Act (FERPA) regarding student records, the CLERY Act regarding campus safety and security, the Health Insurance Portability and Accountability Act (HIPAA) regarding health care patient information, and the Utah Governmental Records Access and Management Act (GRAMA) regarding records of the University as a governmental entity.**
 - c. For purposes of exercising control over the collection, storage, disposal, access, and use of surveillance data, for any surveillance data gathered at any University-controlled space, through any surveillance system operated or controlled by the University, the University considers such data to be the exclusive property of the University of Utah, and not the property of any University employee or contractor.
2. **Restrictions on system placement and operation, and data collection, storage, disposal, access, and use.**
 - a. **Surveillance data may only be collected in compliance with this Policy and associated Regulations, and only through a surveillance system that has been registered with and approved by the SSAC**

(unless exempted). Any collection of surveillance data by any other means is prohibited.

- b. Unless otherwise specifically authorized in advance for a particular compelling purpose by the SSAC and the University General Counsel[, and the Vice President for Administrative Services (or equivalent)]:
 - i. each surveillance system shall include appropriate signage or by other means shall provide reasonable notice of the system's existence, for persons who are subject to the surveillance while present for lawful purposes.
 - ii. no surveillance system shall ever be used to collect video surveillance data from any area which is essentially a *private space*, including the interior space of any restroom, shower or dressing room, lactation room, or individual office of a faculty or staff member, and in the event surveillance data from an essentially public area contains private information, or information to which a reasonable expectation of privacy may attach, such as library records which identify a library patron, such surveillance data should only be reviewed in consultation with the Office of General Counsel; and
 - iii. no surveillance system shall ever be allowed to collect from any location *audio* surveillance data of discernable human voices;

c. Permissible and prohibited uses and purposes for surveillance data.

i. The University may **ordinarily access and use surveillance data only for the limited purposes of deterring, detecting, or investigating criminal activity**, as a means of providing a **campus environment that is safe and secure** for students, employees and visitors visiting for lawful purposes, and protecting University resources and the property of members of the University community from loss or damage.

ii. Further, **under the following restrictions, specifically designated University administrative units may be authorized to have limited access and uses of surveillance data for the following limited types of purposes not limited to criminal activity. Each authorization of such a type of use and purpose must be approved in advance** by the SSAC and the University General

Counsel[[and the Vice President for Administrative Services (or equivalent)]], and only with a specific determination by the SSAC that authorizing the particular type of use is consistent with the basic principles of this Policy, including appropriate protection of individual privacy, and serves a compelling need for the University. **Such an authorization may be made permanently applicable for a defined category of uses by a specified office** as described in a University Procedure, **or may be time-limited as for a specific incident** documented using a form approved by the SSAC. For an administrative investigation of a specific incident, the authorization shall require that access and use of the data be limited only for the purposes of that investigation and only for the time period reasonably necessary. **All such authorizations shall be described in the reports of the SSAC presented periodically to the Academic Senate (without revealing confidential information).**

- a. An administrative investigation of a potential **violation of a non-criminal law or external regulation** which is directly **applicable to the University** or University personnel, if such a violation presents a **substantial risk of serious harm to the University or any individual** (e.g., federal or state regulations regarding storage of controlled substances, or hazardous materials).
- b. An administrative investigation of a potential **violation of a University Regulation** involving a type and degree of non-criminal misconduct which presents a **substantial risk of serious harm to the University or an individual** (e.g., posting racially derogatory materials in a University work- or learning-space to create a hostile work/ learning environment for University employees or students; or operating or storing a wheeled riding device in a dangerous manner or in a prohibited zone).
- c. An administrative investigation by a student-services office regarding a **potential disappearance of a campus-resident student, in circumstances in which the student may be at risk of serious harm** (e.g., a student housing administrator investigating concerns of a minor student's family about the student's well-being after a long period without contact).

- d. A practice of routinely monitoring the presence of University employees or other individuals in specific locations of a facility of the University Hospitals and Clinics, for the limited purposes of protecting patient safety and ensuring compliance with applicable safety regulations.
- e. A practice of routinely monitoring the presence of University employees or other individuals in specific locations of a University facility with restricted access, in circumstances in which such monitoring is necessary to comply with directly applicable external laws and regulations or University Regulations such as for protection of sensitive data or regulated technology, or control of special materials (e.g., University Policy 4-004 Information Security; Policy 7-007 Export Control Compliance; Policy 3-300 University Health and Safety).

iii. The University will not access or use surveillance data (from building access systems or other surveillance systems) for the purposes of

(a) monitoring an individual student's compliance with course attendance requirements, or

(b) monitoring an individual employee's compliance with workplace attendance expectations (except as may be specifically authorized for safety or regulatory compliance purposes in a specific facility under section ii-d or e above).

iv. The University will not use a surveillance system for monitoring the movements or otherwise tracking the location of any individual member of the University community except for the limited purposes authorized under III-C-2-c-i & ii above, or in compliance with a search warrant or any judicially recognized exceptions to warrant requirements.

v. The University will not use facial recognition computer software or equivalent information technology to process video surveillance data to track the presence at a campus location of a particular person for any purpose other than addressing criminal

activity which presents a substantial risk of serious harm to the University or an individual (e.g., a credible threat of a terrorist attack by an identifiable individual at a high-population event on campus).

vi. The University may also use certain anonymized surveillance data for limited administrative purposes of identifying typical patterns of use of University facilities, to aid in design and planning of the campus environment (such as designing pedestrian walkways to best accommodate pedestrian traffic flow in observed high traffic areas). Such uses must be approved by the SSAC in advance on a case-by-case basis, and only with appropriate safeguards for privacy of individuals.

vii. Any other uses of surveillance data by the University shall be allowed only for the limited purposes and to the limited extent required by applicable federal, state, or local law, and each such use shall, to the full extent allowed under that applicable law, be promptly reported to the SSAC with an explanation of its purpose and legal justification.

viii. Targeting individuals based on race, ethnicity, disability, gender, nationality, religion, or other protected classifications in collecting and using surveillance data is prohibited.

~~iv. University will not use facial recognition computer software or equivalent information technology to process video surveillance data to track the presence at a campus location of a particular person;~~

~~v. the University will not use a [video?] surveillance system for monitoring the movements or otherwise tracking the location of any individual member of the University community except in compliance with a search warrant or any judicially recognized exceptions to warrant requirements;~~

~~vi. The University will not use data from building access systems or surveillance systems to monitor an individual student's compliance with course attendance requirements or an individual employee's compliance with workplace attendance expectations.~~

- c. For surveillance systems in areas that are ordinarily used only by particular small groups of University personnel (such as a building section primarily used only by faculty and students of one small academic department), the University encourages that representatives of those regular users of the area be consulted**

about the initial installation or substantial modification of features of such a surveillance system.

d. **The following requirements apply for persons *operating* surveillance systems or otherwise having regular *access to* surveillance data.**

i. **Ordinarily, only University employees** qualified in accord with SSAC-approved criteria shall operate surveillance systems or access surveillance data.

1. Electronic Access Control operators must be University employees appointed by Approving Officers (as defined above).
2. Surveillance system operators must be University employees appointed by Approving Officers.
3. Access to surveillance data shall be granted only to University employees so authorized by the SSAC, and only for purposes approved in accord with this Policy.
4. A list of University employee positions and individuals qualified for these responsibilities will be maintained in the SSAC's registry of systems (see Part III-B above).

ii. **If approved in advance by the SSAC, a particular surveillance system over which the University has authority may be operated by non-University personnel,** in circumstances in which the University contracts with a vendor to provide such system operating services at a specific facility not located on the University's main campus. For example, the SSAC may approve operation of such a system at a distant facility occupied by a University field research station, or a unit of the Hospitals and Clinics. For each such vendor-operated system through which surveillance of members of the University community regularly occurs: (a) the system shall be registered with and approved by the SSAC (unless expressly exempted in accord with Part III-B-2-c of this Policy); (b) the system shall be operated in accord with all relevant provisions of this Policy other than the requirement of operation solely by University personnel (except any provision expressly excluded by the SSAC); and (c) the arrangement with the vendor shall be described in a written contract between the University and the vendor filed with the SSAC.

e. **All video** surveillance data must be stored only on a secure server.

The ~~video~~ data shall be retained only for the specified retention period for that type of surveillance system (as approved by the SSAC and specified in a University Procedure), and after expiration of that period the data shall be deleted, unless it is marked and saved for an approved purpose. Deletion shall ordinarily occur through an automatic erasure process. ~~A~~ The SSAC shall specify a permissible retention period for each type of ~~video~~ surveillance data and each type of surveillance system, which the SSAC shall determine shall be determined based on the camera's surveillance system's location and the system's purpose. The retention periods for centrally operated main systems shall be specified in a University Procedure approved by the SSAC. The retention period for each other (dispersed) system shall be described in the ~~application~~ for documentation of the registration and approval of the system by the SSAC.

f. Bookmarking or saving surveillance data beyond the specified retention period may only be performed by an approved system administrator, and may only be done with specific approval from the SSAC, which approval shall be granted only on a case-by-case basis and only for purposes permitted under this Policy.

~~g. The surveillance data gathered by a centrally operated building access control system (currently the C-Cure system), which consists of logs of entry to a particular space by any person using a particular identity card, does not have a retention period, and so may be retained indefinitely but typically will be retained for no less than 1 year. This data may only be used for purposes approved under this Policy.~~

~~h. (i) The University will ordinarily use surveillance data only for purposes of crime detection and deterrence, to provide a campus environment that is safe and secure for students, employees and visitors visiting for lawful purposes, and to protect University resources from loss or damage. (Drafting Note — To be further discussed — Public Safety dept may recommend considering this be expanded to allow for investigating misconduct that is of very serious concern to the University, but is technically not defined as a crime under Utah law. E.g., could add phrase that “may be used for formal administrative investigations.”)~~

~~(ii) The University may also use certain anonymized surveillance data for limited administrative purposes of identifying typical patterns of use of University facilities, to aid in design and planning of the campus environment (such as designing pedestrian walkways to best accommodate pedestrian traffic flow in observed high traffic areas). Such uses must be approved by the SSAC in advance on a case-by-case basis, and only with appropriate safeguards for privacy of individuals.~~

~~(iii) Any other uses of surveillance data by the University shall be allowed only for the limited purposes and to the limited extent required by applicable federal, state, or local law, and each such use shall, to the full extent allowed under that applicable law, be reported to the SSAC with an explanation of its purpose and legal justification.~~

~~The University will not use data from building access systems or surveillance systems to monitor an individual student's compliance with course attendance requirements or an individual employee's compliance with workplace attendance expectations.~~

~~i. Targeting individuals based on race, ethnicity, disability, gender, nationality, religion, or other protected classifications in collecting and using surveillance data is prohibited.~~

j. The University will release surveillance data to a non-University agency or person (such as a law-enforcement agency) only to the limited extent the University is required to under the terms of the

Utah Government Records Access and Management Act (GRAMA), or other directly applicable state, federal, or local law.

- i. When releasing surveillance data in compliance with GRAMA or other such applicable law, the University will to the full extent permissible under such law protect the privacy of individual members of the University community and visitors visiting for lawful purposes. In particular, the University will protect privacy of students by complying with any applicable requirements of the Family Educational Rights and Privacy Act (FERPA) for any release of surveillance data regarding a student.**
 - ii. Unless prohibited from doing so by the applicable law, the University will: make reasonable efforts to give notice of the planned release to any individual member of the University community who is an identifiable subject of the surveillance data involved; allow such person an opportunity to comment regarding the planned release; and accommodate any lawful reasonable request for managing the release so as to best protect that individual's privacy. In particular the University will comply with applicable pre-release notification requirements of the Family Educational Rights and Privacy Act (FERPA) regarding student records.**
- k. An individual member of the University community who seeks to access and use surveillance data from the University for purposes of conducting *academic research* will ordinarily be required to submit a request through the GRAMA process for obtaining University records. The request will be subject to the same restrictions and requirements as a request made by a non-University party. Additionally, any use of such data involving research with human subjects will be subject to University requirements for such research, which may include review by the Institutional Review Board.**
- l. University personnel who misuse surveillance data or facilitate the misuse of surveillance data by another person are subject to discipline under applicable University Regulations, including provisions of the Student Code, the Faculty Code, or the Corrective Action and Termination Policy for Staff Employees. Such misuse may also be subject to criminal penalties or civil liability under applicable law. The University may audit any surveillance system at any time to detect improper system operation or misuse of data.**

3. Other criteria.

The installation and operation of each building access system and each surveillance system must be consistent with design standards approved by the SSAC. Those design standards must include provisions ensuring appropriate security of the surveillance data, which provisions shall be consistent with [Policy 4-004: University of Utah Information Security Policy](#), and University Rules associated with that Policy.

~~[[**Drafting note:** former contents, to be entirely deleted. —Policy 3-234: Key Policy. Revision 5.~~

~~I. Purpose~~

~~To outline policy and Procedures for issuance and control of door and locker keys for all campus departments and organizations, except student apartments (USA), University Hospital, clinics, and affiliated facilities, and other organizations granted specific exemption by the Vice President for Administrative Services.~~

~~II. Definitions~~

- ~~A. Grand Master Key — A key that activates all door locks in a building.~~
- ~~B. Master Key — A key that activates all door locks in a building for spaces assigned to a specific department.~~
- ~~C. Sub-Master Key — A key that activates the locks in more than one but not all doors to spaces assigned to a specific department.~~
- ~~D. Building Entrance Key — A key that activates the lock only on one or more outside entrance doors to a building.~~
- ~~E. Room Key — A key that activates the lock only to the door to a single room.~~
- ~~F. Locker Key — A key that activates the locks to storage lockers.~~
- ~~G. Approving Officer — A university officer holding the position of department head or higher rank.~~
- ~~H. Designee — A full-time university employee appointed by an approving officer to act in his/her behalf. No more than two may be appointed in any one department.~~

~~III. Policy~~

~~A. Building Security~~

- ~~1. Administrative, college and departmental offices of the university generally are open to the public from 8:00 am to 5:00 pm, Monday through Friday. Certain offices and departments are open at other times to meet particular needs.~~
- ~~2. It is the responsibility of all personnel using buildings after regular hours to see that lights are turned off in the rooms they are vacating and that office doors and outside doors are secured.~~
- ~~3. The Security Officer will investigate night use of all buildings to ascertain whether persons in the buildings are so authorized.~~
- ~~4. Personnel should use all precautions in maintaining the highest level of security to protect university property.~~
- ~~5. To facilitate the security of university buildings and property, keys to offices and buildings may be obtained from Facility Operations Key Shop upon written request from dean or department head. No deposit is required. Deans and department heads are responsible for all keys issued to their department and should assure that keys are returned whenever personnel leave the employment of the university.~~

~~B. Key Issuance~~

~~1. Door Keys. Door keys shall be issued and controlled by the Key Shop.~~

~~a. Duplication of keys, other than by the Key Shop, is prohibited. Any person who knowingly makes or duplicates a university key in any matter not authorized by this policy is subject to disciplinary action by the university, pursuant to established Procedures and/or prosecution in accordance with 1953 Utah Code Annotated, Section 63-9-22 (misdemeanor).~~

~~b. Persons to whom keys are issued shall use the keys only in accordance with this policy.~~

~~2. Limitations. Door keys shall be issued by the Key Shop only upon receipt of a properly completed Application for Keys form. The form must be signed by the applicant, and have the approval signature of the applicant's next higher level of supervisory authority, normally a Dean, Chair, Director or designee.~~

~~a. Grand master keys will not be issued to individuals, except staff in Public Safety, Environmental Health & Safety, and Facility Operations, when 1) a demonstrated need exists, and 2) the cognizant director approves the exception. The Assistant Vice President for Facilities or his/her designee will have the final rights of approval in such cases.~~

~~b. Master keys will be issued only to deans and department heads or to administrative officers of equivalent or higher rank.~~

~~c. Sub-master keys will be issued only to persons authorized to be entrusted with such keys by deans, department heads or administrative officers of equivalent or higher rank.~~

~~d. Building entrance keys will be issued only to persons with a demonstrated need for after hours access to a building.~~

~~e. Room keys will be issued only to persons who have a continuing need for access to such rooms.~~

~~f. A department head may be provided with one extra key for occasional use by subordinates, in which case the department head must assume responsibility for the use of the key.~~

~~g. Keys will not be issued to companies from the private sector working on campus except as specifically pre-authorized in writing by the Assistant Vice President for Facilities or his/her designee. (Refer to section IV.E. for key issuance policy regarding construction and remodeling contractors.)~~

~~C. Key Return~~

~~When an individual's need for a key no longer exists, whether as a result of termination of employment or other reasons, it is the responsibility of the employee's home department to collect the unneeded key(s) from the employee and return it/them to the Key Shop. For reasons of security and data control, it is prohibited for any department to reassign any key from one individual to another without routing the appropriate key request through the Key Shop, as described in Section III.F of this policy.~~

~~D. Responsibilities of Department of Public Safety~~

~~1. The Department of Public Safety is responsible for locking and unlocking building entrance doors at specified times each day. Administrators or departments occupying space within buildings are responsible for locking and unlocking departmentally assigned space.~~

~~2. Individuals who have not been issued keys may gain access to locked buildings and rooms by requesting Public Safety to unlock doors, if there is a bona fide reason for entrance and a current university identification card is shown to the Public Safety officer.~~

~~E. Exceptions~~

~~Exceptions to the policy on issuance of keys may be authorized in writing by the Vice President for Administrative Services.~~

~~F. Procedures~~

~~1. Key Issuance~~

~~a. Individuals wishing to have a key or keys issued to them shall complete an Application for Keys form. The form must be signed by the applicant and the cognizant approving officer or designee, and sent to Facility Operations' Key Shop.~~

~~b. The Key Shop will maintain a file of "Authorized Signatures for Keys" to be used as a basis for key issuance. Keys will be issued only after the signatures on applications for keys have been verified as to authenticity.~~

~~c. The Key Shop will notify departments when keys are ready to be picked up, normally within 24 hours after receipt of the application.~~

~~d. When keys are picked up a copy of the application form will be given to the requesting department for its files.~~

~~2. Key Replacement~~

~~To replace a lost or broken key, an Application for Keys form must be completed in the same manner as for issuance of an original key (see III.F.1. above).~~

~~a. A broken key to be replaced must be returned with the application form.~~

~~b. If a key has been lost, available details must be provided.~~

~~c. If a lost key is later found, it must be returned to the Key Shop.~~

~~3. Locker Keys~~

~~The issuance and control of locker keys is the responsibility of the dean, department head or administrative officer who is charged with control of lockers within a given building.~~

~~4. Record Keeping~~

~~The Key Shop shall maintain a comprehensive listing of all door keys issued by name of individual and department. The section of the listing applicable to a department is available to that department upon request. On an annual basis, Facility Operations will provide each department with a list of keys issued to their department personnel. Such lists shall be returned to the Key Shop after verification for accuracy.~~

~~5. Access to Buildings by Outside Contractors~~

~~a. The Campus Design and Construction Department is responsible for making arrangements with outside contractors requiring building access, and shall coordinate all lock work through the Key Shop.~~

~~b. The Campus Design and Construction Department may, with the written approval of the director of Facility Operations, provide keys to contractors and workmen who have need for access to buildings and rooms being remodeled.~~

~~6. Lock Repair and Replacement~~

~~Locks may not be installed, repaired or replaced on any doors without the specific approval of Facility Operations. Departments will be liable for any resultant damage or costs of corrections if unauthorized installations are made.~~

[Note: Parts IV-VII of this Regulation (and all other University Regulations) are Regulations Resource Information – the contents of which are not approved by the Academic Senate or Board of Trustees, and are to be updated from time to time as determined appropriate by the cognizant Policy Officer and the Institutional Policy Committee, as per [Policy 1-001](#) and [Rule 1-001](#).]

IV. Rules, Procedures, Guidelines, Forms, and other related resources.

- A. Rules
Rule 3-234A: Building Access and Surveillance Systems
- B. Procedures
- C. Guidelines
- D. Forms
- E. Other Related Resource Materials

V. References

[Policy 1-011: Campus Security](#)

[Procedure P1-011A: Campus Security](#)

[University Rule 4-004F: Physical and Facility Security](#)

_____ *{{Drafting note: will need to add references to other U Policies that address related topics, including, eg.,: Policy 1-011 [campus safety---Clery Act] ; Policy 1-012: University Non-discrimination Policy; Policy 3-210: Facility Operations/Maintenance; }}*

VI. Contacts

The designated contact officials for this Policy are:

- A. Policy Owners (primary contact persons for questions and advice):

- a. Systems: _____ ??Executive Director of Facilities Management, ~~Cory D Higgins~~ cory.higgins@fm.utah.edu ~~801-581-5082~~

- b. Data: Chief of Police, Dale Brophy dale.brophy@dps.utah.edu 801-585-2677.

- B. Policy Officers: VP for Administrative Services, John Nixon john.nixon@utah.edu 801-585-0806.

These officials are designated by the University President or delegee, with assistance of the Institutional Policy Committee, to have the following roles and authority, as provided in University Rule 1-001:

"A 'Policy Officer' will be assigned by the President for each University Policy, and will typically be someone at the executive level of the University (i.e., the President and his/her Cabinet Officers). The assigned Policy Officer is authorized to allow exceptions to the Policy in appropriate cases... ."

"The Policy Officer will identify an "Owner" for each Policy. The Policy Owner is an expert on the Policy topic who may respond to questions about, and provide interpretation of the Policy; and will typically be someone reporting to an executive level position (as defined above), but may be any other person to whom the President or a Vice President has delegated such authority for a specified area of University operations. The Owner has primary responsibility for maintaining the relevant portions of the Regulations Library... [and] bears the responsibility for determining which reference materials are helpful in understanding the meaning and requirements of particular Policies... ." University Rule 1-001-III-B & E.

VII. History

A. Current version: Revision 7.

Approved by the Academic Senate [date].

Approved by the Board of Trustees [date].

[Revision 6](#): Approved by Board of Trustees April 12, 2011, Adding text removed from Policy 4-005 Rev. 4, see Executive Summary. Also reformatted to comply with format standards.

Legislative history for Revision 6: [Memorandum February, 11, 2011](#).

[Revision 5](#): Approved July 8, 1996

B. Earlier versions: Beginning with Revision #7, this replaces former Policy 3-234 Key Policy.

University Rule 3-234A: Building Access and Surveillance Systems. Revision 0.

Effective Date: [Upon final approval]

I. Purpose and Scope:

A. Purpose: This Rule implements University Policy 3-234 Building Access and Surveillance Systems. The purposes of this Rule are to regulate the installation and operation of building access systems (including building key systems and electronic access and associated management interfaces), regulate the installation and operation of surveillance systems, and regulate the collection, storage, and use of surveillance data collected through system surveillance systems for University buildings and outdoor areas.

B. Scope: This Rule applies to all persons on University property.

This Rule regulates building access systems and surveillance systems with a *primarily fixed location* at a University building or outdoor area.

II. Definitions:

The definitions in University Policy 3-234 apply for purposes of this Rule.

III. Rule:

A. Administrative responsibility and funding for Building Access and Surveillance Systems.

1. Administrative responsibility for systems.

a. Departments operating surveillance systems registered with and approved by the Surveillance Systems Administrators Committee (SSAC) are responsible for the installation, management, maintenance, and use of surveillance software (which ordinarily will be carried out by the department's designated Information Technology staff). **And see Policy 3-234-III-B-2-b, prohibiting the operation of any system which has not been registered and approved, unless exempted.**

b. Each surveillance system monitoring activity in an area which has been designated by the DPS as a Public Safety Space will ordinarily be centrally managed, by the Campus Building Access Team.

2. Funding of Systems.

- a. Initial acquisition and installation costs and renovations of both building access systems and surveillance systems are funded through various sources apart from ongoing operations and maintenance.
- b. After initial installation, the designated [Facility Steward] for a building ordinarily manages the operation and maintenance, and routine replacement of building access systems and surveillance systems for that building, funded through per-device fees and other fund allocations within the purview of the [Facility Steward].
- c. The Campus Building Access Team reviews actual costs and projections annually for the operations and maintenance of Electronic Access Control and Surveillance Systems and proposes fee adjustments. The Vice President for Administrative Services approves such adjustments.
- d. Devices providing electronic access or surveillance for areas designated as Public Safety Spaces, and other areas ordinarily used by the general public, are funded from the General Fund. Other devices are funded by the department using those devices. Departments are responsible for damage and costs resulting from unauthorized installations.

B. Registration and Approval of Surveillance Systems.

1. The following exemptions from the otherwise applicable surveillance system registration requirements of Policy 3-234-III- are hereby granted.
 - a. Clinical Patient Care.
Monitoring patients under medical care by authorized medical professionals.
 - b. Human Subject Research.
Research authorized by the Institutional Review Board for Human Subject Research.
 - c. Teaching and Learning.
Recording for instructional purposes as part of an approved University of Utah course, under supervision of the course instructor.
 - d. Video Conferencing.
Meetings conducted through electronic devices where all parties are aware of being recorded.
 - e. Personal Communication Devices (i.e., smart phones) and Others, as specified by the SSAC.

C. Key Systems.

1. A key system consists of mechanical locks and keys, including master keys.
2. Each building key system for a University facility must meet campus design standards and be approved by the applicable Facility Steward.
3. Initial key systems, including keys for the initial set of authorized users, are ordinarily provided in conjunction with the construction or renovation project, with costs for the keys included in the project costs.
4. Replacements for lost keys are provided by the Campus Building Access Team, with replacement costs billed to the requesting department. Replacements for broken or faulty keys which are returned are replaced at no cost to the requesting department.
5. If a University-owned or -occupied facility has been identified as a “security risk” such that changing locks becomes necessary, then the building occupant responsible for the risk is liable for the resulting costs. The SSAC, along with input from Risk Management and Property Accounting, will determine whether a facility is such a security risk. Considerations in this determination may include, but are not limited to:
 - a. number or type of keys unaccounted for or lost;
 - b. theft or vandalism risk;
 - c. life safety concerns;
 - d. sensitive, technical, proprietary, or high-value equipment.
6. Departments are required to account for keys annually, or as requested by the Campus Building Access Team or the Department of Public Safety.
7. Departments are responsible for returning keys when access is no longer required.
8. All key users (persons to whom any key is issued) must be approved by an Approving Officer (as defined in Policy 3-234) or their designee.

9. Prior to authorizing keys, an Approving Officer or designee must have completed the University-authorized access security training within the past two years.
10. Master keys are issued to individuals only upon receiving the appropriate authorization. The level of required authorization is based on the type of master key, as follows:

Type of Master Key:	Authorization Required From:
a. Master Keys Covering Multiple Buildings and/or Electronic Access Override Keys	Surveillance System Administrators Committee (SSAC)
b. Building Master for Multi-Department Building	Cognizant Vice President for Each Department
c. Building Master for Single Department Building and/or Department Master within Multi-Department Building	Approving Officer
d. Other Keys (Building Entrances, Department Sub-Master, Offices, etc.)	Approving Officer or Authorized Representative

[Note: Parts IV-VII of this Regulation (and all other University Regulations) are Regulations Resource Information – the contents of which are not approved by the Academic Senate or Board of Trustees, and are to be updated from time to time as determined appropriate by the cognizant Policy Officer and the Institutional Policy Committee, as per [Policy I-001](#) and [Rule I-001](#).]

IV. Procedures, Guidelines, Forms, and other related resources. [Reserved]

V. References

- a. Policy 3-234 Building Access and Surveillance Systems.

VI. Contacts

The designated contact officials for this Rule are:

- A. Policy Owners (primary contact persons for questions and advice):

~~a. Systems: Executive Director of Facilities Management, Cory D Higgins
cory.higgins@fm.utah.edu 801-581-5082~~

- b. Data: Chief of Police, Dale Brophy dale.brophy@dps.utah.edu 801-585-2677.
- B. Policy Officers: VP for Administrative Services, John Nixon john.nixon@utah.edu 801-585-0806.

These officials are designated by the University President or delegee, with assistance of the Institutional Policy Committee, to have the following roles and authority, as provided in University Rule 1-001:

"A 'Policy Officer' will be assigned by the President for each University Policy, and will typically be someone at the executive level of the University (i.e., the President and his/her Cabinet Officers). The assigned Policy Officer is authorized to allow exceptions to the Policy in appropriate cases... ."

"The Policy Officer will identify an "Owner" for each Policy. The Policy Owner is an expert on the Policy topic who may respond to questions about, and provide interpretation of the Policy; and will typically be someone reporting to an executive level position (as defined above), but may be any other person to whom the President or a Vice President has delegated such authority for a specified area of University operations. The Owner has primary responsibility for maintaining the relevant portions of the Regulations Library... [and] bears the responsibility for determining which reference materials are helpful in understanding the meaning and requirements of particular Policies... ."
University Rule 1-001-III-B & E.

VII. History

- A. Current version:

University Rule 3-234A, Revision 0. Approved by the Academic Senate [date] .
Approved by the Board of Trustees: [date], with the designated effective date of [____].

Legislative history of Revision 0. {upload & link to proposal presented to Academic Senate & Trustees}

- B. Earlier versions: [Reserved].

University Procedure 3-234A

Registration and Approval of Building Access Systems and Surveillance Systems

To implement University Policy 3-234 and University Rule 3-234A, as enacted [January 2019].

Approved by the Surveillance System Administrators Committee (SSAC), date_____

[EXAMPLE ONLY FOR DISCUSSION PURPOSES--- DRAFT 2018-12-28]

I. Overall timetable for initial registration and approval, and periodic renewal reviews, of the various systems.

Phase 1. All systems are to be *initially inventoried* by _____[date]. Inventorying occurs by system operators providing to the SSAC a brief general description using the SSAC approved form. Being merely included in this inventory does not constitute SSAC approval of any system as meeting the criteria under Policy 3-234 for continuing operation.

Phase 2. Groups of systems begin approval process, on staggered deadlines. The SSAC organizes the previously inventoried list of systems into appropriate groupings, develops a series of staggered deadlines, assigns a time period for the operators of the systems in each group to submit an application for approval, and notifies the operators of their timelines. Organizing the systems into groups with staggered timelines allows the SSAC to do its review work at a reasonable pace, rather than having the entire list of systems arriving for review in one brief period. The SSAC may also find that these groupings will be useful for setting staggered timelines for required renewals of registration & approvals in subsequent years. E.g., systems in one group might be scheduled to undergo a renewal review two years from the original, another group in the third year, etc, so that the renewal work for the SSAC will be staggered and paced, rather than having the reviews of every system occur at the same time. Some flexibility on this scheduling is best left to the SSAC to adapt as it learns from experience in the first years of operating the registry.

Phase 3. Systems, by groups, on established dates, are considered for approval by the SSAC, and approved if criteria are met. For noncompliant systems, efforts are made to correct deficiencies, and if compliance is ultimately not attained those systems are shut down. System operators complete and submit their approval applications according to the staggered schedule (using SSAC approved form). The SSAC reviews applications, and for those systems which meet the established criteria, they are placed on the approved registry and permitted to continue operating (until their scheduled renewal review). For any system which has an incomplete application, or otherwise fails to meet criteria, the SSAC withholds approval, and attempts to work with system operators to correct deficiencies. If satisfaction of approval criteria can eventually be demonstrated, SSAC will register the system as approved and schedule it for the appropriate renewal period. If the SSAC determines that any system will not be brought into

compliance with the approval criteria within a reasonable time, the SSAC will deny approval, categorize it accordingly on the registry, and require that operation of the system be ceased.

Phase 4. Renewal reviews are scheduled and conducted. All systems after initial approval and listing on the registry are required to go through a summary renewal review process no less frequently than every [five] years. On the staggered schedule set by the SSAC, and using an SSAC-approved renewal application form using then-current approval criteria, each system’s operator applies for renewal. The SSAC reviews, approves renewal of compliant systems, and works with operators to correct deficiencies of non-compliant systems (or requires shut-down of systems which are not made compliant within reasonable time).

The SSAC may also choose to do spot checks of compliance of any systems, at any time, including at the time of scheduled renewal. And any member of the University community concerned about improper operation of any system or misuse of surveillance data may at any time recommend to SSAC that it review a particular system. SSAC has the authority and discretion to review any system at any time, including auditing the automated records of access to stored data, and the authority to require any non-compliant system to be brought into compliance or to cease operation— subject only to appeal to the Vice President for Administrative Services, whose decision is final, as per Policy 3-234.

[Note that by provisions in Policy 3-234, a full report on the implementation of the revised Policy and the registration & approval process will be presented to the Academic Senate by {October 2020}. And on an ongoing basis beginning 2019 there are to be annual summary reports to the Senate on the activities of the SSAC.]

II. Checklist of criteria for approval of surveillance systems at time of initial approval, and on renewal for continuing operation.

___ Compliant with all applicable federal, state, and local laws (including FERPA, Clery, HIPAA and GRAMA).

Compliant with Policy 3-234 requirements, including:

___ system meets SSAC-approved system design standards

___ adequate signage or other appropriate means of notifying surveilled persons of the existing of the surveillance (e.g., signs indicating presence of cameras. Balancing sufficient number and visibility of signs, without undue expense for the University).

___ qualifications of system operators/persons with routine access to data

___ security of data storage servers and otherwise secure handling of data

___ data retention period & assured deletion of aged-out data appropriate for the particular type of system (see standard periods in this Procedure below)

____ restrictions on bookmarking or saving data beyond ordinary retention period

____ restrictions on collecting audio data, data from essentially private spaces (e.g. individual faculty offices), & private information from otherwise essentially public areas

____ history of and continuing commitment to allowing only proper uses of collected data (crime detection & deterrence, safety & security, [[or other SSAC approved limited administrative purpose]]).

----- other specific criterion approved by the SSAC, consistent with principles of Policy 3-234.
Describe & explain_____.

____ Overall, consistency with Policy 3-234 underlying principles of protecting privacy of individuals to fullest extent possible while providing safe & secure campus environment.

III. Retention periods for stored surveillance data, based on the type of surveillance system and use of such data.

The following are the maximum periods that stored surveillance data may ordinarily be retained. Any exception of saving data longer than this period must be approved in advance by the SSAC, either through approval of the system plan at time of registration, or approval for a specific instance case-by-case.

Type of system

Ordinary maximum retention period

[EXAMPLE--TBD]

[EXAMPLE --TBD]



Safe Campus – the role of Video Surveillance ?



Campus guardians are looking out for you !

Building Access & Surveillance Systems Policy

Status quo:

- **20+ year old policy** (mechanical lock & key only)
- **modern tech:** Electronic Access Systems & Video Surveillance Systems= greatly increase Safety & Security, but Privacy Concerns
 - Some large systems **centrally managed** by DPS;
 - numerous **smaller dispersed** building-specific systems
 - Little central oversight, regs on storage & use of data
 - **not even good inventory yet !**
- **no clear regulations:** installing Surveillance Systems, who runs, how Data stored, **permissible & prohibited Uses.**

Building Access & Surveillance Systems Policy

= need revised Regulations

- Combination: main Policy, initially one Rule (later add other specific Rules, & very detailed Procedures).
 - Start with “fixed-location” systems– later tackle issues of “mobile” (e.g., drones, body-cams)
- Guiding Principles:
 - enhance Campus Safety & Security,
 - respect Privacy,
 - Notice, Transparency, Consultation,
 - must follow Federal & State Law.

Background-- Federal & State laws

- Campus safety— e.g., Clery Act
- Privacy: e.g., FERPA (student records). HIPAA (patient privacy).
- **GRAMA: Utah Government Records Access Management Act.**
 - UU is “*governmental entity,*” w/ “*government records*”
 - Very specific rules on how UU responds to requests (from individuals, law enforcement agencies, news media, etc.)
 - Specific –limited-- bases for *withholding* (entire records, or redacting specific information, e.g., blur out faces in videos).

Building Access & Surveillance Systems Policy

Initiative's main Elements:

- *new*-- Oversight Committee (“SSAC”).
- *new* – Registration, Approval, Review process.
- *new*-- Criteria for: access & surveillance systems; data storage.
- *new*– Set *permissible* and *prohibited uses* of surveillance data (& grant rare **exceptions**).
- *continue but improve* –regulating, tracking, safeguarding **mechanical locks & keys**.

main Elements

- Oversight Committee (“SSAC”).
 - **Members**= Faculty, Student, Staff & Administration reps (Facilities, Public Safety, Gen-Counsel, etc.).
 - Flesh out approval *criteria*, develop & oversee registration & review *processes*.
- Registration, Approval, periodic Review Processes (for systems & operators).
 - create Central Registry, conduct Initial Inventory of multitude of smaller systems.
 - Apply criteria for initial *approvals*, periodic *reviews*.

main Elements

- **Criteria for:** building access & surveillance systems; secure data storage; operator personnel training, & auditing.
 - Baseline of fundamentals set now by Senate & Trustees in Policy 3-234.
 - Further details developed by oversight committee SSAC, set in formal Rules & Procedures.
- ... Criteria include adherence to restrictions on *uses* of surveillance data

main Elements

- *Permissible & Prohibited uses* of surveillance data.
 - Fundamental *principles & normal* rules set by Senate & Trustees now in Policy 3-234.
 - Process for circumstantially-justified granting of rare *exceptions*.
- **Balance:** (1) adequately protect persons & property (criminal activity: physical assaults, property theft & damage). (2) Respect privacy, individual autonomy, academic freedom.
(3) follow Law.

Timeline—phases 1-4

- 1: Enact Basic Regulations- Senate & Trustees.
- 2: Form SSAC oversight committee, develop & implement registration & approval process.
- 3: by [2020] report to Senate with startup period experience, propose further revising Reg's as needed.
- 4: Consider reg's other topics—e.g., mobile surveillance drones & body cameras; special events.

(Near term Concern: Utah Legislative Audit--USHE institutions. UU response at least Phase 1 in place before January legislature session.)

Senate Exec. Committee--**ad hoc drafting group:**

Faculty from Sen. Executive Committee:

- Prof. Bob Flores—Senate Policy Liaison (Law) robert.flores@law.utah.edu
- Prof. Randy Dryer-- EC member (Law, Honors)
- Prof. Leslie Francis—EC member (Law, Philosophy, Medicine)
- Senate Officers – Tom Richmond (Chemistry), Julio Facelli (Medicine), Mardie Clayton (Nursing)

Student from ASUU:

- Devon Cantwell

Administration/ staff From Facilities Management & Public Safety:

- Dept. of Public Safety—Chief of Police-- Dale Brophy
- Facilities Management—Exec. Director-- Cory Higgins, Assoc. Director --Joseph Ashurst.
- Contact: Exec Assistant—Karen Janicki karen.janicki@utah.edu

Others consulted:

- Office of General Counsel-- Robert Payne, Michelle Ballantyne
- Office of VP Academic Affairs-- Harriet Hopf
- Office of VP Health Sciences --Bob Fujinami
- Institutional Policy Committee (representatives of: Human Resources, Staff Council, Budget & Planning, Finance, Hospitals & Clinics, Information Technology, VP Research)